Research in Cloud Security and Privacy
--Security and Privacy Issues in Cloud Computing

Portions of this PPT draw from PPTs authored by Bharat Bhargava, Anya Kim and YounSun Cho

ASU ARIZONA STATE UNIVERSITY

Outline

- Part I: Introduction
- Part II: Security and Privacy Issues in Cloud Computing
- Part III: Possible Solutions

Part III. Possible Solutions

- Minimize Lack of Trust
  - Policy Language
  - Certification
- Minimize Loss of Control
  - Monitoring
  - Utilizing different clouds
  - Access control management
  - Identity Management (IDM)
- Minimize Multi-tenancy

Security Issues in the Cloud

- In theory, minimizing any of the issues would help:
  - Third Party Cloud Computing
  - Loss of Control
    - Take back control
      - Data and apps may still need to be on the cloud
      - But can they be managed in some way by the consumer?
  - Lack of trust
    - Increase trust (mechanisms)
      - Technology
      - Policy, regulation
      - Contracts (incentives): topic of a future talk
  - Multi-tenancy
    - Private cloud
      - Takes away the reasons to use a cloud in the first place
    - VPC: its still not a separate system
    - Strong separation

Known issues: Already exist

- Confidentiality issues
- Malicious behavior by cloud provider
- Known risks exist in any industry practicing outsourcing
- Provider and its infrastructure needs to be trusted

New Vulnerabilities & Attacks

- Threats arise from other consumers
- Due to the subtleties of how physical resources can be transparently shared between VMs
- Such attacks are based on placement and extraction
- A customer VM and its adversary can be assigned to the same physical server
- Adversary can penetrate the VM and violate customer confidentiality

More on attacks…

- Collaborative attacks
- Mapping of internal cloud infrastructure
- Identifying likely residence of a target VM
- Instantiating new VMs until one gets co-resident with the target
- Cross-VM side-channel attacks
- Extract information from target VM on the same machine

7

More on attacks…

- Can one determine where in the cloud infrastructure an instance is located?
- Can one easily determine if two instances are co-resident on the same physical machine?
- Can an adversary launch instances that will be co-resident with other user instances?
- Can an adversary exploit cross-VM information leakage once co-resident?

Answer: Yes to all

8

Minimize Lack of Trust

9

Minimize Lack of Trust: Policy Language

- Consumers have specific security needs but don't have a say-so in how they are handled
  - What the heck is the provider doing for me?
  - Currently consumers cannot dictate their requirements to the provider (SLAs are one-sided)
- Standard language to convey one's policies and expectations
  - Agreed upon and upheld by both parties
  - Standard language for representing SLAs
  - Can be used in a intra-cloud environment to realize overarching security posture

10

Minimize Lack of Trust: Policy Language (Cont.)

- Create policy language with the following characteristics:
  - Machine-understandable (or at least processable),
  - Easy to combine/merge and compare
  - Examples of policy statements are, "requires isolation between VMs", "requires geographical isolation between VMs", "requires physical separation between other communities/tenants that are in the same industry," etc.
  - Need a validation tool to check that the policy created in the standard language correctly reflects the policy creator's intentions (i.e. that the policy language is semantically equivalent to the user's intentions).

11

Minimize Lack of Trust: Certification

- Certification
  - Some form of reputable, independent, comparable assessment and description of security features and assurance
  - Sarbanes-Oxley, DIACAP, DISTCAP, etc (are they sufficient for a cloud environment?)
- Risk assessment
  - Performed by certified third parties
  - Provides consumers with additional assurance

12

Minimize Loss of Control

Minimize Loss of Control: Monitoring

- Cloud consumer needs situational awareness for critical applications
  - When underlying components fail, what is the effect of the failure to the mission logic
  - What recovery measures can be taken (by provider and consumer)
- Requires an application-specific run-time monitoring and management tool for the consumer
  - The cloud consumer and cloud provider have different views of the system
  - Enable both the provider and tenants to monitor the components in the cloud that are under their control

Minimize Loss of Control: Monitoring (Cont.)

- Provide mechanisms that enable the provider to act on attacks he can handle.
  - infrastructure remapping (create new or move existing fault domains)
  - shutting down offending components or targets (and assisting tenants with porting if necessary
  - Repairs
- Provide mechanisms that enable the consumer to act on attacks that he can handle (application-level monitoring).
  - RAdAC (Risk-adaptable Access Control)
  - VM porting with remote attestation of target physical host
  - Provide ability to move the user's application to another cloud

Minimize Loss of Control: Utilize Different Clouds

- The concept of 'Don't put all your eggs in one basket'
  - Consumer may use services from different clouds through an intra-cloud or multi-cloud architecture
  - Propose a multi-cloud or intra-cloud architecture in which consumers
    - Spread the risk
    - Increase redundancy (per-task or per-application)
    - Increase chance of mission completion for critical applications
  - Possible issues to consider:
    - Policy incompatibility (combined, what is the overarching policy?)
    - Data dependency between clouds
    - Differing data semantics across clouds
    - Knowing when to utilize the redundancy feature (monitoring technology)
    - Is it worth it to spread your sensitive data across multiple clouds?
      - Redundancy could increase risk of exposure

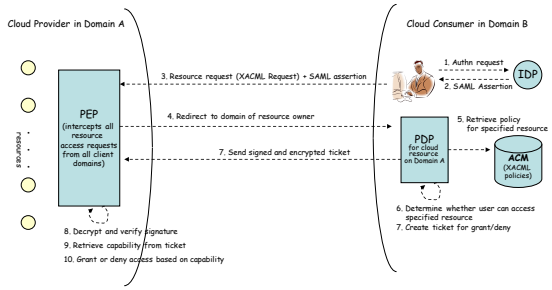
Minimize Loss of Control: Access Control

- Many possible layers of access control
  - E.g. access to the cloud, access to servers, access to services, access to databases (direct and queries via web services), access to VMs, and access to objects within a VM
  - Depending on the deployment model used, some of these will be controlled by the provider and others by the consumer
- Regardless of deployment model, provider needs to manage the user authentication and access control procedures (to the cloud)
  - Federated Identity Management: access control management burden still lies with the provider
  - Requires user to place a large amount of trust on the provider in terms of security, management, and maintenance of access control policies. This can be burdensome when numerous users from different organizations with different access control policies, are involved

Minimize Loss of Control: Access Control (Cont.)

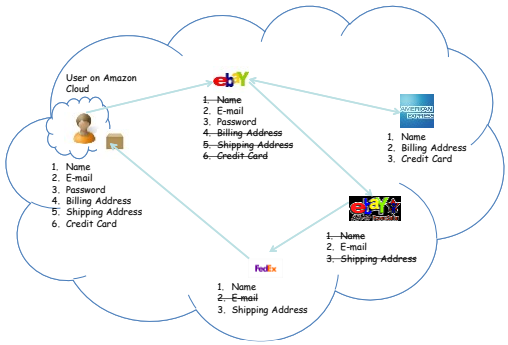
- Consumer-managed access control
  - Consumer retains decision-making process to retain some control, requiring less trust of the provider (i.e. PDP is in consumer's domain)
  - Requires the client and provider to have a pre-existing trust relationship, as well as a pre-negotiated standard way of describing resources, users, and access decisions between the cloud provider and consumer. It also needs to be able to guarantee that the provider will uphold the consumer-side's access decisions.
  - Should be at least as secure as the traditional access control model.
  - Facebook and Google Apps do this to some degree, but not enough control
  - Applicability to privacy of patient health records

Minimize Loss of Control: Access Control



Minimize Loss of Control: IDM Motivation

Minimize Loss of Control: IDM Identity in the Cloud



Minimize Loss of Control: IDM Present IDMs

- IDM in traditional application-centric IDM model
  - Each application keeps track of identifying information of its users.
- Existing IDM Systems
  - Microsoft Windows CardSpace [W. A. Alrodhan]
  - OpenID [http://openid.net]
  - PRIME [S. F. Hubner]

These systems require a **trusted third party** and do not work on an **untrusted host**.

If Trusted Third Party is compromised, all the identifying information of the users is also compromised

[Latest: **AT&T iPad leak**]

Minimize Loss of Control: IDM Issues in Cloud Computing

- Cloud introduces several issues to IDM
  - Users have **multiple accounts** associated with **multiple service providers.**
  - Lack of trust
    - o Use of Trusted Third Party is not an option
    - o Cloud hosts are untrusted
  - Loss of control
    - o Collusion between Cloud Services
      - – Sharing sensitive identity information between services can lead to undesirable **mapping of the identities to the user.**

IDM in Cloud needs to be user-centric

Minimize Loss of Control: IDM Goals of Proposed User-Centric IDM for the Cloud

1. Authenticate without disclosing identifying information
2. Ability to securely use a service while on an untrusted host (VM on the cloud)
3. Minimal disclosure and minimized risk of disclosure during communication between user and service provider (Man in the Middle, Side Channel and Correlation Attacks)
4. Independence of Trusted Third Party

Minimize Loss of Control: IDM Approach - 1

- **IDM Wallet:**
  - Use of AB scheme to protect PII from untrusted hosts.
- **Anonymous Identification:**
  - Use of Zero-knowledge proofing for authentication of an entity without disclosing its identifier.

25

Minimize Loss of Control: IDM Components of Active Bundle (Approach – 1)

- **Identity data:** Data used during authentication, getting service, using service (i.e. SSN, Date of Birth).
- **Disclosure policy:** A set of rules for choosing Identity data from a set of identities in IDM Wallet.
- **Disclosure history:** Used for logging and auditing purposes.
- **Negotiation policy:** This is Anonymous Identification, based on the Zero Knowledge Proofing.
- **Virtual Machine:** Code for protecting data on untrusted hosts. It enforces the disclosure policies.

26

Minimize Loss of Control: IDM Anonymous Identification (Approach – 1)

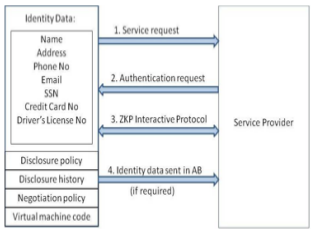
Anonymous Identification

(Shamir's approach for Credit Cards)

- IdP provides Encrypted Identity Information to the user and SP.
- SP and User interact
- Both run IdP's public function on the certain bits of the Encrypted data.
- Both exchange results and agree if it matches.

27

Minimize Loss of Control: IDM Usage Scenario (Approach – 1)



28

Minimize Loss of Control: IDM Approach - 2

- Active Bundle scheme to protect PII from untrusted hosts
- Predicates over encrypted data to authenticate without disclosing unencrypted identity data.
- Multi-party computing to be independent of a trusted third party

29

Minimize Loss of Control: IDM Usage Scenario (Approach – 2)

- Owner O encrypts Identity Data(PII) using algorithm Encrypt and O's public key PK. Encrypt outputs CT—the encrypted PII.
- SP transforms his request for PII to a predicate represented by function p.
- SP sends shares of p to the n parties who hold the shares of MSK.
- n parties execute together KeyGen using PK, MSK, and p, and return TKp to SP.
- SP calls the algorithm Query that takes as input PK, CT, TKp and produces p(PII) which is the evaluation of the predicate.
- The owner O is allowed to use the service only when the predicate evaluates to "true".

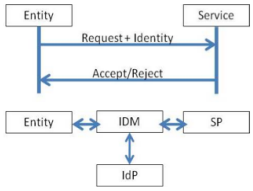
30

Minimize Loss of Control: IDM
Representation of identity information

- Token/Pseudonym
- Identity Information in clear plain text
- **Active Bundle**

31

Minimize Loss of Control: IDM
Motivation-Authentication Process using PII



Problem: Which information to disclose and how to disclose it.

32

Proposed IDM: Mechanisms

- [16] *Protection of Identity Information in Cloud Computing without Trusted Third Party* - R. Ranchal, B. Bhargava, L.B. Othmane, L. Lilien, A. Kim, M. Kang, Third International Workshop on Dependable Network Computing and Mobile Systems (DNCMS) in conjunction with 29th IEEE Symposium on Reliable Distributed System (SRDS) 2010
- [17] *A User-Centric Approach for Privacy and Identity Management in Cloud Computing* - P. Angin, B. Bhargava, R. Ranchal, N. Singh, L. Lilien, L.B. Othmane 29th IEEE Symposium on Reliable Distributed System (SRDS) 2010
- *Privacy in Cloud Computing Through Identity Management* - B. Bhargava, N. Singh, A. Sinclair, International Conference on Advances in Computing and Communication ICACC-11, April, 2011, India.

- Active Bundle
- Anonymous Identification
- Computing Predicates with encrypted data
- Multi-Party Computing
- Selective Disclosure

33

Proposed IDM: Active Bundle

- Active bundle (AB)
  - An encapsulating mechanism protecting data carried within it
  - Includes data
  - Includes metadata used for managing confidentiality
    - o Both privacy of data and privacy of the whole AB
  - Includes Virtual Machine (VM)
    - o performing a set of operations
    - o protecting its confidentiality

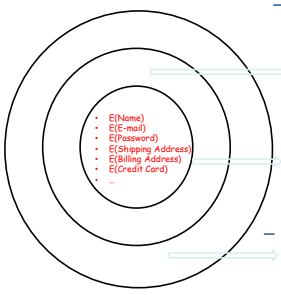
34

Proposed IDM: Active Bundle (Cont.)

- Active Bundles—Operations
  - Self-Integrity check
    E.g., Uses a hash function
  - Evaporation/ Filtering
    Self-destroys (a part of) AB's sensitive data when threatened with a disclosure
  - Apoptosis
    Self-destructs AB's completely

35

Proposed IDM: Active Bundle Scheme



– Metadata:
- Access control policies
- Data integrity checks
- Dissemination policies
- Life duration
- ID of a trust server
- ID of a security server
- App-dependent information
- …

– Sensitive Data:
- Identity Information
- …

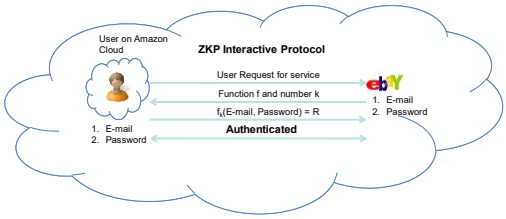
– Virtual Machine (algorithm):
- Interprets metadata
- Checks active bundle integrity
- Enforces access and dissemination control policies
- …

* E( ) - Encrypted Information

36

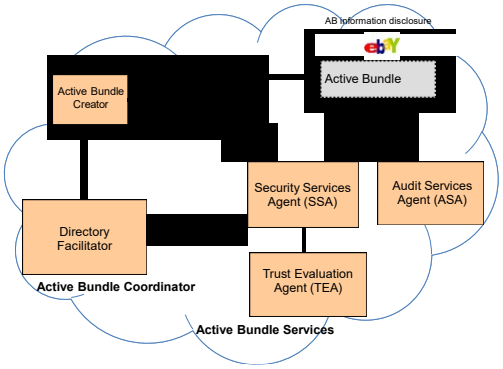
Proposed IDM: Anonymous Identification

- Use of Zero-knowledge proofing for user authentication without disclosing its identifier.



37

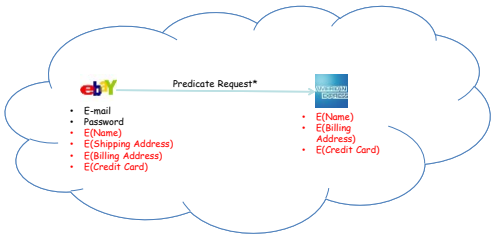
Proposed IDM: Interaction using Active Bundle



38

Proposed IDM: Predicate over Encrypted Data

- Verification without disclosing unencrypted identity data.

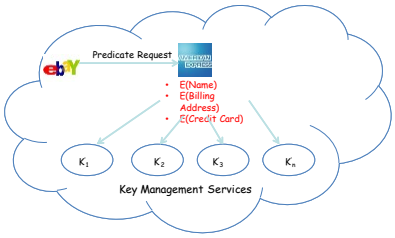


*Age Verification Request
*Credit Card Verification Request

39

Proposed IDM: Multi-Party Computing

- To become independent of a trusted third party
  - Multiple Services hold shares of the secret key
  - Minimize the risk

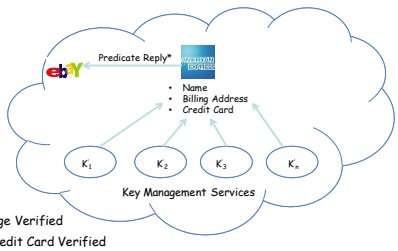


* Decryption of information is handled by the Key Management services

40

Proposed IDM: Multi-Party Computing

- To become independent of a trusted third party
  - Multiple Services hold shares of the secret key
  - Minimize the risk

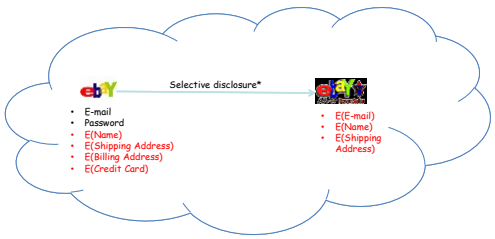


*Age Verified
*Credit Card Verified

41

Proposed IDM: Selective Disclosure

- User Policies in the Active Bundle dictate dissemination

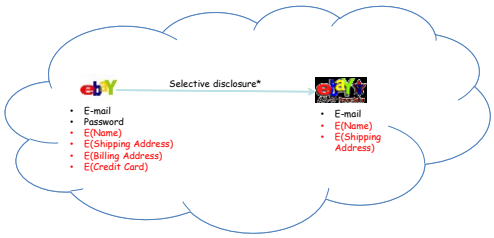


*e-bay shares the encrypted information based on the user policy

42

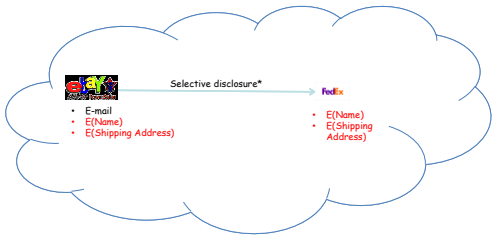
Proposed IDM: Selective Disclosure

- User Policies in the Active Bundle dictate dissemination



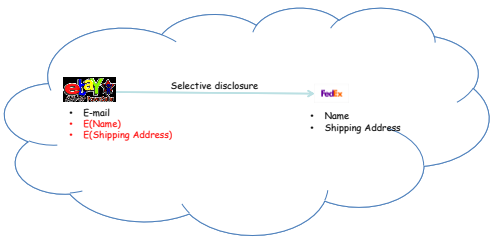
Decryption handled by Multi-Party Computing as in the previous slides

Proposed IDM: Selective Disclosure



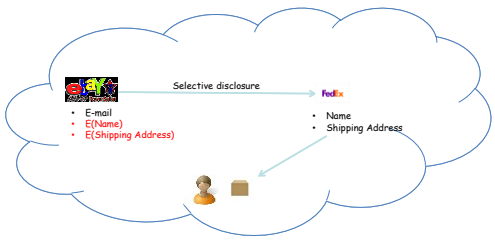
*e-bay seller shares the encrypted information based on the user policy

Proposed IDM: Selective Disclosure



- Decryption handled by Multi-Party Computing as in the previous slides

Proposed IDM: Selective Disclosure



- Fed-Ex can now send the package to the user

Proposed IDM: Identity in the Cloud

Proposed IDM: Characteristics and Advantages

- Ability to use Identity data on untrusted hosts
  - Self Integrity Check
  - Integrity compromised- apoptosis or evaporation
  - Data should not be on this host
- Independent of Third Party
  - Prevents correlation attacks
- Establishes the trust of users in IDM
  - Through putting the user in control of who has his data
  - Identity is being used in the process of authentication, negotiation, and data exchange.
- Minimal disclosure to the SP
  - SP receives only necessary information.

Proposed IDM: Conclusion & Future Work

- Problems with IDM in Cloud Computing
  - Collusion of Identity Information
  - Prohibited Untrusted Hosts
  - Usage of Trusted Third Party
- Proposed Approaches
  - IDM based on Anonymous Identification
  - IDM based on Predicate over Encrypted data
- Future work
  - Develop the prototype, conduct experiments and evaluate the approach

49

Minimize Multi-tenancy

50

Minimize Multi-tenancy

- Can't really force the provider to accept less tenants
  - Can try to increase isolation between tenants
    - Strong isolation techniques (VPC to some degree)
      - C.f. VM Side channel attacks (T. Ristenpart et al.)
    - QoS requirements need to be met
    - Policy specification
  - Can try to increase trust in the tenants
    - Who's the insider, where's the security boundary? Who can I trust?
    - Use SLAs to enforce trusted behavior

51

Conclusion

- Cloud computing is sometimes viewed as a reincarnation of the classic mainframe client-server model
  - However, resources are ubiquitous, scalable, highly virtualized
  - Contains all the traditional threats, as well as new ones
- In developing solutions to cloud computing security issues it may be helpful to identify the problems and approaches in terms of
  - Loss of control
  - Lack of trust
  - Multi-tenancy problems

52

What did they do?

- Proposed identity-based authentication for cloud computing, based on the identity-based hierarchical model for cloud computing (IBHMCC) and corresponding encryption and signature schemes
- Being certificate-free, the authentication protocol aligned well with demands of cloud computing

Identity-Based Authentication for Cloud Computing

Hongwei Li, Yuanshun Dai, Ling Tian, and Haomiao Yang

CloudCom '09

ASU ARIZONA STATE UNIVERSITY

54

Identity-Based Hierarchical Model for Cloud Computing (IBHMCC)

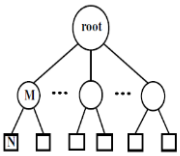


Fig. 1. IBHM for cloud computing

- Define the identity of node is the DN string from the root node to the current node itself.
- The identity of entity N is ID_N = DN_0 || DN_M || DN_N

55

Deployment of IBHMCC

- Root PKG setup and Low-level setup

Root PKG setup: Root PKG acts as follows:

1. Generate group G_1, G_2 of some prime order q and an admissible pairing $\hat{e}: G_1 \times G_1 \to G_2$;
2. Choose an arbitrary generator $P \in G_1$;
3. Choose cryptography hash functions $H_1: \{0,1\}^* \to G_1, H_2: G_2 \to \{0,1\}^n$ for some n;
4. Pick a random $\alpha \in \mathbb{Z}_q^*$ and set $Q_0 = \alpha P$, $P_0 = H_1(DN_0), S_0 = \alpha P_0$. The root PKG's master key is S_0 and the system parameters are $< G_1, G_2, \hat{e}, Q_0, P, P_0, H_1, H_2 >$.

56

Deployment of IBHMCC (cont.)

Lower-level setup

1. Assume there are m nodes in the level-1. For each node, the root PKG acts as follows (let X be an arbitrary node in the m nodes):
2. Compute the public key of node $X: P_X = H_1(ID_X)$, where $ID_X = DN_0 \| DN_X$;
3. Pick the secret point $\rho_X \in \mathbb{Z}_q^*$ for node X. ρ_X is only known by node X and its parent node;
4. Set the secret key of node $X: S_X = S_0 + \rho_X P_X$;
5. Define the Q-value: $Q_{ID_X\|} = \rho_X P$. $Q_{ID_X\|}$ is public.

- After that, all nodes in the level-1 get and securely keep their secret keys and the secret points.
- The public key and the Q-value are publicized.
- Then, Each node in the level-1 similarly repeats the above steps (2-5).

57

Identity-Based Encryption

Encryption: Assume E_1 and E_2 are two entities in the cloud computing. The identity of entity E_2 is $ID_{E_2} = DN_0 \| DN_1 \| DN_2$. To encrypt message m with ID_{E_2}, E_1 acts as follows:

1. Compute

$$P_1 = H_1(DN_0 \| DN_1) \quad (1)$$

$$P_2 = H_1(DN_0 \| DN_1 \| DN_2) \quad (2)$$

2. Choose a random $r \in \mathbb{Z}_q^*$;
3. Output the ciphertext

$$C = < rP, rP_1, rP_2, H_2(g^r) \oplus m > \quad (3)$$

where $g = \hat{e}(Q_0, P_0)$ which can be pre-computed.

58

Identity-Based Encryption (cont.)

Decryption: After receiving the ciphertext $C = < U_0, U_1, U_2, V >$, entity E_2 can decrypt C using its secret key $S_{E_2} = S_0 + \rho_1 P_1 + \rho_2 P_2$, where ρ_1 is the secret point of node $DN_0 \| DN_1$, ρ_2 is the secret point of node $DN_0 \| DN_1 \| DN_2$:

1. Compute

$$d = \frac{\hat{e}(U_0, S_{E_2})}{\prod_{i=1}^{2} \hat{e}(Q_{ID_{E_2}i}, U_i)} \quad (4)$$

where $Q_{ID_{E_2}1} = \rho_1 P, Q_{ID_{E_2}2} = \rho_2 P$;

2. Output the message $m = H_2(d) \oplus V$.

59

Identity-Based Signature

Signature: To sign message m, entity E_2 acts as follows:

1. Compute $P_m = H_1(DN_0 \| DN_1 \| DN_2 \| m)$;
2. Compute $\delta = S_{E_2} + \rho_2 P_m$, where ρ_2 is the secret point of entity E_2;
3. Output the signature $< \delta, P_m, Q_{ID_{E_2}1}, Q_{ID_{E_2}2} >$.

Verification: Other Entities can verify the signature by acting as follows: Confirm

$$\hat{e}(P, \delta) = \hat{e}(P, \rho_2 P_m)\ \hat{e}(Q_0, P_0) \prod_{i=1}^{2} \hat{e}(Q_{ID_{E_2}i}, P_i) \quad (5)$$

if the equation is true, the signature is validated.

60

Identity-Based Authentication for

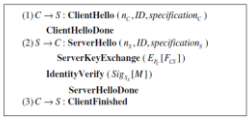


Fig. 2. Identity-based Authentication Protocol

where

n_c, n_s : the fresh random number
ID : the session identifier
$specification_c$: the cipher specification of C
$specification_s$: the cipher specification of S
F_{CS} : a pre-master secret used to generate the shared key
$E_{P_C}[F_{CS}]$: encrypt F_{CS} with the public key P_C of entity C using the encryption algorithm of IBE
M : all handshake messages since the ClientHello message
$Sig_{S_S}[M]$: sign M with the private key S_S of entity S using the signature algorithm of IBS

·Extends from TLS to handle the IBE and IBS schemes

61

A Simple Technique for Securing Data at Rest Stored in a Computing Cloud

Jeff Sedayao, Steven Su, Xiaohao Ma, Minghao Jiang, and Kai Miao

CloudCom '09

ASU ARIZONA STATE UNIVERSITY

What did they do?

- Simple technique implemented with Open Source software solves the confidentiality of data stored on Cloud Computing Infrastructure by using public key encryption to render stored data at rest unreadable by unauthorized personnel, including system administrators of the cloud computing service on which the data is stored
- Validated their approach on a network measurement system implemented on PlanetLab
- Used it on a service where confidentiality is critical – a scanning application that validates external firewall implementations

63

Problem Scope

- Goal is to ensure the confidentiality of data at rest
- "Data at rest" means that the data that is stored in a readable form on a Cloud Computing service, whether in a storage product like S3 or in a virtual machine instance as in EC2

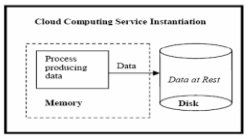


Fig. 1. Process in a Cloud Computing Infrastructure producing Data at Rest

64

Problem Scope (cont.)

- To protect data at rest, they want to prevent other users in the cloud infrastructure who might have access to the same storage from reading the data our process has stored
- They also want to prevent system administrators who run the cloud computing service from reading the data.
- They assume that it is unlikely for an adversary to snoop on the contents of memory.
  - If the adversary had that capability, it is unlikely that we could trust the confidentiality of any of the data that we generated there.

65

Problem Scope (cont.)

- While the administrative staff of the cloud computing service could theoretically monitor the data moving in memory before it is stored in disk, we believe that administrative and legal controls should prevent this from happening.
- They also do not guard against the modification of the data at rest, although we are likely to be able to detect this.

66

Solution Design

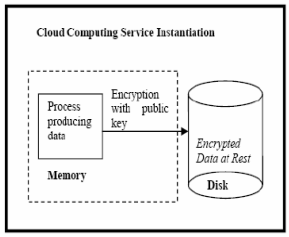


Fig. 2. Process in a Cloud Computing Infrastructure producing Encrypted Data at Rest

67

Solution Design (cont.)

- On a trusted host, collect the encrypted data, as shown in Figure 3, and decrypt it with the collection agent's private key which stays on that host. Note that in this case, we are in exclusive control of the private key, which the cloud service provider has no view or control over.
- They will discuss this feature of our solution later.

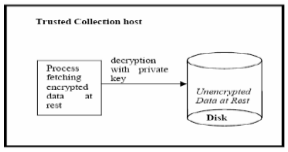


Fig. 3. Process in a Cloud Computing Infrastructure producing Encrypted Data at Rest

68

Implementation Experiences

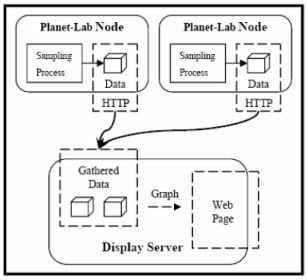


Fig. 4. Web performance data gathering and display methodology

69

Implementation Experiences (cont.)

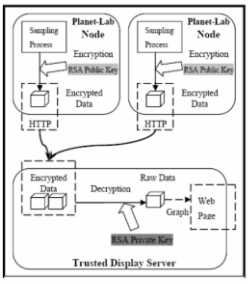


Fig. 5. Secured Web Performance Monitoring Application with Data Encryption and Decryption

70

Privacy in a Semantic Cloud: What's Trust Got to Do with It?

Åsmund Ahlmann Nyre and Martin Gilje Jaatun
CloudCom'09

What did they do?

- A brief survey on recent work on privacy and trust for the semantic web, and sketch a middleware solution for privacy protection that leverages probabilistic methods for automated trust and privacy management for the semantic web

Trust Management

- Definition of trust
  - The willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor and control that other party.

73

Trust Management (cont.)

- Trust Models
  - Mayer, R., Davis, J., Schoorman, F.: An integrative model of organizational trust. Academy of Management Review
    - The main factors of trustworthiness were identified as ability, benevolence and integrity.
    - On the trustor's part, disposition to trust and perceived risk were identified as the most influential factors with regards to trust.
    - Furthermore, the outcome of a trust relation (experience) is assumed to influence one or more of the trustworthiness factors and hence the trustworthiness of the trustee.

74

Trust Management (cont.)

- Trust Models
  - The complexity of several proposed models does not necessarily give better trust assessments
  - Conrad, M., French, T., Huang, W., Maple, C.: A lightweight model of trust propagation in a multi-client network environment: to what extent does experience matter?
    - Proposed a lightweight model for trust propagation. The parameters self confidence, experience, hearsay and prejudice are used to model and assess trust. This computational model also allows agents to compute a trust value to automatically perform trust decisions.

75

Trust Management (cont.)

- Trust Models
  - Gil, Y., Artz, D.: Towards content trust of web resources
    - The idea is to arrive at content trust, where the information itself is used for trust calculation.
    - This allows for a whole new range of parameters (such as bias, criticality, appearance, etc.) to be used when assessing trust in resources.
    - The problem of such parameters is that they require user input, which conflicts with the assumption of agents conducting the assessment autonomously.

76

Trust Management (cont.)

- Trust Propagation
  - Golbeck, J., Hendler, J.: Accuracy of metrics for inferring trust and reputation in semantic web-based social networks
    - Inferring trust and reputation in social networks when entities are not connected directly by a trust relationship.
    - Done by computing the weighted distance from the source to the sink.
    - Any distrusted entity is not included in the computation since the trust assessments done by such entities are worthless.

77

Trust Management (cont.)

- Trust Propagation
  - Guha, R., Kumar, R., Raghavan, P., Tomkins, A.: Propagation of trust and distrust
    - Introduce the notion of distrust to address the problem of expressing explicit distrust as a contrast to the absence of trust.
    - Absence of trust may come from lack of information to conduct a proper trust assessment, while distrust expresses that a proper assessment have been conducted and that the entity should not be trusted.
    - Furthermore, they argue that distrust could also be propagated and proposes several propagation models in addition to trust transitivity, including co-citation, which is extensively used for web searches.

78

Trust Management (cont.)

- Trust Propagation
  - Huang, J., Fox, M.S.: An ontology of trust: formal semantics and transitivity
    - o claim that not all kinds of trust can be assumed to be transitive.
    - o They note that trust based on performance, i.e. an entity performing as expected repeatedly, is not necessarily transitive, while trust based on a belief that the entity will perform as expected often is.

79

Probabilistic Privacy Policy

- A probabilistic approach to policy enforcement, where users are given a probability that their requirements will be respected and polices enforced.
- Thus when interacting with websites who are known to be less trustworthy, policy adherence is given by a probability metric that the website will actually enforce its own policies.
- This enforcement model does not include a privacy or trust model
  - o i.e. it is only occupied with how to handle uncertainty in enforcement and provide a tool for interacting with non-conforming entities while minimizing the risks involved.

80

Probabilistic Privacy Policy Enforcement (cont.)

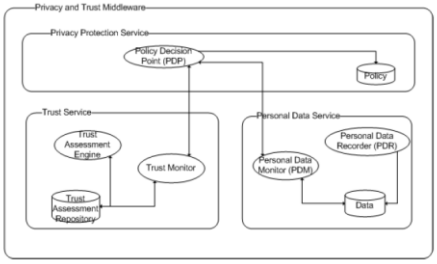


Fig. 1. Middleware architecture for probabilistic privacy management

81

Probabilistic Privacy Policy Enforcement (cont.)

- Personal Data Recorder (PDR)
  - Protecting users from this kind of aggregation requires complete control of what information has been distributed and to whom.
  - Records what data is transmitted to which receivers.
    - o Example: Consider the situation where a user wanting to stay unidentified has provided his postal code and anonymous e-mail address to a website. Later he also provides age and given name (not the full name) and the anonymous e-mail address. Now, the website is able to combine the data (postal code, age and given name) to identify the anonymous user
      - The second interaction with the website should have been blocked, since it enables the website to reveal the user's identity. The PDR allows the user to view himself through the eyes of the receiving party, and thereby perform aggregation to see whether too much information is provided.

82

Probabilistic Privacy Policy Enforcement (cont.)

- Personal Data Monitor (PDM)
  - Computing and assessing policies and behaviour, and to update the personal data recorder with inferred knowledge.
  - Determine the likelihood that the personal information distributed to the receiver will also reach other.
    - o Example: sending an e-mail with a business proposition to a specific employee of a company, it is likely that other employees in that company also will receive the e-mail (e.g. his superior).
    - o PDM is responsible for inferring other recipients and to include such information in the Personal Information Base.
    - o Hence, any interaction later on should consider this information when assessing the kind of information to reveal.

83

Probabilistic Privacy Policy Enforcement (cont.)

- Trust Assessment Engine (TAE)
  - Calculating trust values of different entities in order to determine their trustworthiness.
  - The TAE is focused solely on assessing communicating parties and does not take into account risk willingness, vulnerability and criticality.

84

Probabilistic Privacy Policy Enforcement (cont.)

- Trust Monitor (TM)
  - Detecting events that might affect the perceived trustworthiness and the willingness to take risks.
  - Calculating and deciding on what is an acceptable trust level, given the circumstances.
  - Any computed trust value and feedback received from cooperating entities is stored in the trust assessment repository

85

Probabilistic Privacy Policy Enforcement (cont.)

- Policy Decision Point (PDP)
  - The final decision on whether to engage in information exchange and if so; under what conditions.
  - Collects the views of both the TM and the PDM and compares their calculations to the policies and requirements found in the policy repository.
  - The decision is reported back to the TM and PDM to allow recalculation in case the decision alters the calculated trust values or distribution of personal information

86

Towards an Approach of Semantic Access Control for Cloud Computing

Luokai Hu, Shi Ying, Xiangyang Jia, and Kai Zhao
CloudCom'09

ASU ARIZONA STATE UNIVERSITY

What did they do?

- Analysis existing access control methods and present a new Semantic Access Control Policy Language (SACPL) for describing Access Control Policies (ACPs) in cloud computing environment.
- Access Control Oriented Ontology System (ACOOS) is designed as the semantic basis of SACPL.
- Ontology-based SACPL language can effectively solve the interoperability issue of distributed ACPs.

88

Access Control Oriented Ontology System (ACOOS)

- Provide the common understandable semantic basis for access control in cloud computing environments.
- Divided into four parts, Subject Ontology, Object Ontology, Action Ontology and Attribute Ontology
- Web Ontology Language (OWL) is selected as the modeling language of ACOOS.
  - Ontology is helpful to construct authorization policy within the scope of whole cloud computing environment based on policy definition elements with determined semantics.

89

Access Control Oriented Ontology System (ACOOS)

- Subject Ontology
  - Subject is the entity that has a number of action permissions over object.
    - o e.g., a user, a user group, an organization, a role, a process, a service
  - Attribute of a subject is described by the data property
  - The role in subject ontology represents the capability of a subject to implement a task.
  - Access permission of resources can be encapsulated in the role.
    - o If a subject is assigned to a role, it can access the resources indirectly.

90

Access Control Oriented Ontology System (ACOOS)

- Object Ontology
  - Object is the entity as receptor of action and is need for protection.
    - o e.g., data, documents, services and other resources.
  - Attribute of an object is described by the data property and object property of OWL with hasObjectDataAttribute and hasObjectAttribute respectively.
  - Object group can also be used to define the rule to organize objects.
    - o Each object group in fact establishes a new object concept, all object individuals of the object concept have object attribute values of the object group.

91

Access Control Oriented Ontology System (ACOOS)

- Action Ontology
  - With the cloud computing technology, usually a large number of subjects and objects but only a relatively small number of actions could be found
    - o e.g., such as reading, writing and execution
  - Action also has properties, known as the ActionAttribute, which describes various information of action for authorization and management.
  - Action group can be defined with helpful for the definition of rules.
    - o The definition of action group, nearly the same with the object group, will not repeat it again.

92

Access Control Oriented Ontology System (ACOOS)

- Attribute Ontology
  - Attribute types are defined in the attribute ontology, can be used to define the attribute of almost all entities, including the subject, object and action.
  - The attribute value of entities is often needed to determine whether meet the Permit conditions or Deny ones.

93

Semantic Access Control Policy Language (SACPL)

- Policy markup language, such as XACML, supports description and management of distributed policies.
- The ACP of an object (resource) may be completed by a number of departments even organizations, such as information systems department, human resources and financial department.
- The same ACP may be applied to the internal network protection, e-mail system, remote access systems, or a cloud computing platform.
- As a result, in cloud computing environment, the issue of interoperability among policies is more important than ever before.

94

References

1. NIST (Authors: P. Mell and T. Grance), "The NIST Definition of Cloud Computing (ver. 15)," National Institute of Standards and Technology, Information Technology Laboratory (October 7 2009).
2. J. McDermott, (2009) "Security Requirements for Virtualization in Cloud Computing," presented at the ACSAC Cloud Security Workshop, Honolulu, Hawaii, USA, 2009.
3. J. Camp. (2001), "Trust and Risk in Internet Commerce," MIT Press
4. T. Ristenpart et al. (2009) "Hey You Get Off My Cloud," Proceedings of the 16th ACM conference on Computer and communications security, Chicago, Illinois, USA
5. Security and Privacy in Cloud Computing, Dept. of CS at Johns Hopkins University. www.cs.jhu.edu/~ragib/sp10/cs412
6. Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance by Tim Mather and Subra Kumaraswamy
7. Afraid of outside cloud attacks? You're missing the real threat. http://www.infoworld.com/d/cloud-computing/afraid-outside-cloud-attacks-youre-missing-real-threat-894
8. **Amazon downplays report highlighting vulnerabilities in its cloud service.** http://www.computerworld.com/s/article/9140174/Amazon_downplays_report_highlighting_vulnerabilities_in_its_cloud_service
9. **Targeted Attacks Possible in the Cloud, Researchers Warn.** http://www.cio.com/article/506136/Targeted_Attacks_Possible_in_the_Cloud_Researchers_Warn
10. **Vulnerability Seen in Amazon's Cloud-Computing by David Talbot.** http://www.cs.sunysb.edu/~sion/research/sion2009mitTR.pdf
11. **Cloud Computing Security Considerations by Roger Halbheer and Doug Cavit. January 2010.** http://blogs.technet.com/b/rhalbheer/archive/2010/01/30/cloud-security-paper-looking-for-feedback.aspx
12. **Security in Cloud Computing Overview.http://www.halbheer.info/security/2010/01/30/cloud-security-paper-looking-for-feedback**
13. **Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds by T. Ristenpart, E. Tromer, H. Shacham and Stefan Savage. CCS'09**
14. **Cloud Computing Security.** http://www.exforsys.com/tutorials/cloud-computing/cloud-computing-security.html
15. **Update From Amazon Regarding Friday's S3 Downtime by Allen Stem. Feb. 16, 2008.** http://www.centernetworks.com/amazon-s3-downtime-update
16. R. Ranchal, B. Bhargava, L.B. Othmane, L. Lilien, A. Kim, M. Kang, "Protection of Identity Information in Cloud Computing without Trusted Third Party," Third International Workshop on Dependable Network Computing and Mobile Systems (DNCMS) in conjunction with 29th IEEE Symposium on Reliable Distributed System (SRDS) 2010
17. P. Angin, B. Bhargava, R. Ranchal, N. Singh, L. Lilien, L.B. Othmane, "A User-Centric Approach for Privacy and Identity Management in Cloud Computing," 29th IEEE Symposium on Reliable Distributed System (SRDS) 2010
18. H. Khandelwal, *et al.*, "Cloud Monitoring Framework," Purdue University. Dec 2010.

95

Other References for Cloud Security

- M. Armbrust, *et al.*, "Above the Clouds: A Berkeley View of Cloud Computing," UC Berkeley Reliable Adaptive Distributed Systems LaboratoryFebruary 10 2009.
- Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing, ver. 2.1," 2009.
- M. Jensen, *et al.*, "On Technical Security Issues in Cloud Computing," presented at the 2009 IEEE International Conference on Cloud Computing, Bangalore, India 2009.
- P. Mell and T. Grance, "Effectively and Securely Using the Cloud Computing Paradigm," ed: National Institute of Standards and Technology, Information Technology Laboratory, 2009.
- N. Santos, *et al.*, "Towards Trusted Cloud Computing," in *Usenix 09 Hot Cloud Workshop*, San Diego, CA, 2009.
- R. G. Lennon, *et al.*, "Best practices in cloud computing: designing for the cloud," presented at the Proceeding of the 24th ACM SIGPLAN conference companion on Object oriented programming systems languages and applications, Orlando, Florida, USA, 2009.
- P. Mell and T. Grance, "The NIST Definition of Cloud Computing (ver. 15)," National Institute of Standards and Technology, Information Technology LaboratoryOctober 7 2009.
- C. Cachin, *et al.*, "Trusting the cloud," *SIGACT News*, vol. 40, pp. 81-86, 2009.
- J. Heiser and M. Nicolett, "Assessing the Security Risks of Cloud Computing," Gartner 2008.
- A. Joch. (2009, June 18) Cloud Computing: Is It Secure Enough? *Federal Computer Week*.
- AWS Amazon EC2: http://aws.amazon.com/ec2/
- Amazon CloudWatch: http://aws.amazon.com/cloudwatch/
- Iperf: http://iperf.sourceforge.net/

96